BY ORDER OF THE
COMMANDER AIR COMBAT COMMAND

ACC DIRECTORY 90-264

27 JULY 2000

Command Policy

COMPLIANCE AND STANDARDIZATION REQUIREMENTS LIST INFORMATION SECURITY PROGRAM MANAGEMENT

OPR: HQ ACC/SFOP
(Mr. Chad D. Lamphere)
OCR: ACC IGS/CC
(Colonel James D. Wessler)
Supersedes ACCDIR 90-264, 21 July 1999

Certified by: HQ ACC/SF
(Colonel Donal J. Collins)

Pages: 5
Distribution: F

This directory implements AFPD 90-2, *Inspector General--The Inspection System*: and ACCI 90-202, *ACC Compliance and Standardization Requirements List (C&SRL) Program*. Table 1 of this directory lists compliance items in support of guidance in DoD 5200.1-R, *Information Security Program*; AFI 31-401, *Information Security Program Management*; and related ACC Supplement 1. These publications provide policy direction to promote proper and effective classification, protection, and downgrading of official information requiring safeguarding in the interest of the national security. Units may supplement this directory to add internal compliance items. It applies to all active ACC units. This directory does not apply to Air National Guard or Air Force Reserve Command units/members. Send comments and suggested improvements to this directory on AF Form 847, **Recommendation for Change of Publication**. Send to HQ ACC/SFO, 220 Sweeney Boulevard, Suite 112, Langley AFB VA 23665-2796.

SUMMARY OF REVISIONS

This document has been substantially revised and should be completely reviewed.

1. General. The items listed do not constitute the order or limit the scope of the inspection/assessment. As a minimum, units should use these directories in conjunction with the annual Unit Self-Assessment. The objective is to identify deficiencies that preclude attainment of required capabilities. Units can supplement this publication to add internal compliance items. Higher headquarters may use this directory in whole or in part during visits or exercises. Users may add any item(s) that, in the exercise of good judgment, requires examination.

1.1. Critical Compliance Objectives (CCO). Items defined by the ACC staff as key result areas for successful mission accomplishment including, but not limited to, items where noncompliance could result in serious injury, loss of life, excessive cost, or litigation. CCOs are shown in **BOLD AND ALL CAPS FORMAT**.

1.2. Core Compliance Items (CCI). Areas that require special vigilance and are important to the overall performance of the unit, but are not deemed "critical." Noncompliance would result in some negative impact on mission performance or could result in injury, unnecessary cost, or possible litigation. CCIs are shown in ALL CAPS FORMAT.

1.3. General Compliance Items (GCI). Areas deemed fundamental to successful overall performance of the unit, but noncompliance would result in minimal impact on mission accomplishment or would be unlikely to result in injury, increased cost, or possible litigation. GCIs are shown in sentence case format.

Table 1. Information Security Program Management.

ITEM NO.	ITEM	REFERENCES
CCO-1	**ARE THE INFORMATION SECURITY PROGRAM MANAGER (ISPM) AND EACH UNIT COMMANDER MANAGING THE INFORMATION SECURITY PROGRAM?**	**AFI 31-401, PARA 1.3.4.1. AND PARA 1.3.5.3.**
1.1.	HAS THE UNIT COMMANDER/STAFF AGENCY CHIEF APPOINTED A SECURITY MANAGER, AND NECESSARY ALTERNATES, TO ENSURE THE INFORMATION SECURITY PROGRAM IS IMPLEMENTED?	AFI 31-401, PARA 1.3.5.1.
1.2.	Are unit security managers maintaining a security manager's handbook as required?	AFI 31-401/ACC Sup 1, para 1.3.6.9.
1.3.	Has a current security manager appointment letter been provided to the ISPM?	AFI 31-401/ACC Sup 1, para 1.3.5.1.
1.4.	IS THE ISPM CONDUCTING ANNUAL PROGRAM REVIEWS FOR THOSE UNITS STORING CLASSIFIED INFORMATION?	AFI 31-401, PARA 1.4.2.
1.5.	Has the unit commander/staff agency chief designated personnel to conduct semiannual security self-inspections?	AFI 31-401, para 1.4.3.
1.6.	IS CLASSIFIED INFORMATION STORED IN GENERAL SERVICES ADMINISTRATION APPROVED SECURITY CONTAINERS OR APPROVED VAULTS OR SECURE ROOMS?	DOD 5200.1-R, PARA 6-402 AND APPENDIX G
1.7.	HAS THE ISPM APPROVED, IN WRITING, THE USE OF VAULTS AND SECURE ROOMS TO STORE CLASSIFIED INFORMATION?	AFI 31-401/ACC SUP 1, PARA 5.20.4.
1.8.	Are all classified items clearly identified to show classification?	DoD 5200.1-R, para 5-100
1.9.	Is a record, i.e., Standard Form (SF) 700, **Security Container Information**, maintained for each vault, secure room, or security container used for storing classified information, showing location of the container, the names, home addresses, and home telephone numbers of the individuals having knowledge of the combination?	DoD 5200.1-R, para 6-404b(3)

ITEM NO.	ITEM	REFERENCES
1.10.	Has a system of security checks at the close of each working day been established to ensure that the area is secure, and is SF 701, **Activity Security Checklist**, and SF 702, **Security Container Check Sheet**, used as part of this system?	DoD 5200.1-R, para 6-302
1.11.	Has the installation commander designated an over-night repository for classified material?	AFI 31-401, para 5.14.1.
1.12.	Has the installation commander authorized the storage of Secret material on the flightline during in processing for deployment?	AFI 31-401, para 5.14.2.
1.13.	Has a Top Secret Control Officer (TSCO) and alternate been designated to maintain the Top Secret Control Account information?	AFI 31-401, para 5.10.1.1.
1.14.	Is an AF Form 143, **Top Secret Register Page**, used to account for all Top Secret documents and AIS material?	AFI 31-401, para 5.10.1.1.
1.15.	Is AF Form 144, **Top Secret Access Record and Cover Sheet**, used as the disclosure record kept with the applicable Top Secret material?	AFI 31-401, para 5.10.1.2.1.
1.16.	IS AN INVENTORY CONDUCTED ANNUALLY OR WHEN THERE IS A CHANGE IN TSCOS?	AFI 31-401, PARA 5.10.1.3.1.
1.17.	Are procedures developed to protect incoming mail delivered by messenger until a determination is made whether classified material is contained in the package?	AFI 31-401, para 5.10.8.
1.18.	ARE PLANS FOR THE PROTECTION, REMOVAL, OR DESTRUCTION OF CLASSIFIED MATERIAL IN CASE OF FIRE, NATURAL DISASTER, CIVIL DISTURBANCE, TERRORIST ACTIVITIES, OR ENEMY ACTION DEVELOPED?	DOD 5200.1-R, PARA 6-303a
1.19.	If used, has the ISPM approved alternate or compensa-tory security controls?	AFI 31-401, para 5.30.1.
1.20.	Are requests for waivers for DoD 5200.1-R and AFI 31-401 sent through ISPM channels to HQ USAF/ XOFI?	AFI 31-401, para 5.30.1.
1.21.	Does the ISPM provide technical guidance and monitor the status of security incidents?	AFI 31-401, para 9.6.1.1. and para 9.6.1.2.
1.22.	HAVE ALL AIR FORCE CLEARED PERSONNEL (MILITARY AND CIVILIAN) EXECUTED AN SF 312, **NONDISCLOSURE AGREEMENT**?	AFI 31-401, PARA 5.5.

ITEM NO.	ITEM	REFERENCES
1.23.	Is AF Form 2587, **Security Termination Statement**, used for personnel termination briefings when separating from the service, terminating civilian employment, or terminating access to special program material?	AFI 31-401, para 8.10.1.
CCO-2	**ARE ORIGINAL CLASSIFICATION AUTHORITIES (OCA) INDOCTRINATED IN THE FUNDAMENTALS OF SECURITY CLASSIFICATION, LIMITATIONS ON THEIR AUTHORITY TO CLASSIFY INFORMATION, AND THEIR RESPONSIBILITIES AS SUCH PRIOR TO THE EXERCISE OF THIS AUTHORITY?**	**DOD 5200.1-R, PARA 2-202**
2.1.	Does the ISPM provide training to OCAs before they exercise their authority?	DoD 5200.1-R, para 2-202; AFI 31-401, para 8.5.
CCO-3	**DOES THE ISPM PROVIDE AND MONITOR TRAINING AS REQUIRED BY AFI 31-401, CHAPTER 8?**	**AFI 31-401, PARA 1.3.4.3.**
3.1.	Are all individuals who are cleared for access to classified information given an initial orientation to the Information Security Program before being allowed access to classified?	DoD 5200.1-R, para 9-200a
3.2.	Has the commander, staff agency chief, and supervisor implemented an effective recurring and refresher security training program?	AFI 31-401, para 8.9.
3.3.	Is refresher training being accomplished at least annually?	DoD 5200.1-R, para 9-401

JOHN P. JUMPER, General, USAF
Commander